Doc. No. 78-5036-01

Installing 6-Port MICA Modules and Carrier Cards in Cisco AS5200 Universal Access Servers

Product Number: AS52-MCC=

This document describes how to replace 6-port MICA modules and carrier cards in Cisco AS5200 universal access servers. The part numbers are as follows:

- MICA carrier card with 24 ports, AS52-24DM-CC=
- MICA carrier card with 30 ports, AS52-30DM-CC=
- 6-port MICA modules, 6DM=

This document includes the following sections:

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Safety Recommendations

Follow these guidelines to ensure general safety:

- Keep the chassis area clear and dust-free during and after installation.
- Keep tools away from walk areas where you or others could fall over them.
- Do not wear loose clothing that could get caught in the chassis. Fasten your tie or scarf and roll up your sleeves.
- Wear safety glasses when working under any conditions that might be hazardous to your eyes.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.

Safety Warnings

Safety warnings appear throughout this publication in procedures that, if performed incorrectly, may harm you. A warning symbol precedes each safety warning.

Warning .Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.

Waarschuwing Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het document *Regulatory Compliance and Safety Information* (Informatie over naleving van veiligheids- en andere voorschriften) raadplegen dat bij dit toestel is ingesloten.

Varoitus Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. Tässä julkaisussa esiintyvien varoitusten käännökset löydät laitteen mukana olevasta *Regulatory Compliance and Safety Information* -kirjasesta (määräysten noudattaminen ja tietoa turvallisuudesta).

Attention Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions d’avertissements figurant dans cette publication, consultez le document *Regulatory Compliance and Safety Information* (Conformité aux règlements et consignes de sécurité) qui accompagne cet appareil.

Warnung Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. Übersetzungen der in dieser Veröffentlichung enthaltenen

Warnhinweise finden Sie im Dokument *Regulatory Compliance and Safety Information* (Informationen zu behördlichen Vorschriften und Sicherheit), das zusammen mit diesem Gerät geliefert wurde.

Avvertenza Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nel documento *Regulatory Compliance and Safety Information* (Conformità alle norme e informazioni sulla sicurezza) che accompagna questo dispositivo.

Advarsel Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i dokumentet *Regulatory Compliance and Safety Information* (Overholdelse av forskrifter og sikkerhetsinformasjon) som ble levert med denne enheten.

Aviso Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. Para ver as traduções dos avisos que constam desta publicação, consulte o documento *Regulatory Compliance and Safety Information* (Informação de Segurança e Disposições Reguladoras) que acompanha este dispositivo.

¡Advertencia! Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. Para ver una traducción de las advertencias que aparecen en esta publicación, consultar el documento titulado *Regulatory Compliance and Safety Information* (Información sobre seguridad y conformidad con las disposiciones reglamentarias) que se acompaña con este dispositivo.

Varning! Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. Se förklaringar av de varningar som förkommer i denna publikation i dokumentet *Regulatory Compliance and Safety Information* (Efterrättelse av föreskrifter och säkerhetsinformation), vilket medföljer denna anordning.

Safety with Electricity

Warning Read the installation instructions before you connect the system to its power source.

Warning Ultimate disposal of this product should be handled according to all national laws and regulations.

Warning Only trained and qualified personnel should be allowed to install or replace this equipment.

Warning Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.

Follow these guidelines when working on equipment powered by electricity:

- Locate the emergency power-OFF switch in the room in which you are working. Then, if an electrical accident occurs, you can quickly shut the power OFF.
- Disconnect all power before doing the following:
  - Installing or removing a chassis
  - Working near power supplies
- Do not work alone if potentially hazardous conditions exist.
- Never assume that power is disconnected from a circuit. Always check.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, and missing safety grounds.
- If an electrical accident occurs, proceed as follows:
  - Use caution; do not become a victim yourself.
  - Turn OFF power to the system.
  - If possible, send another person to get medical aid. Otherwise, determine the condition of the victim and then call for help.
  - Determine if the person needs rescue breathing or external cardiac compressions; then take appropriate action.

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. It occurs when electronic printed circuit cards are improperly handled and can result in complete or intermittent failures. Always follow ESD prevention procedures when removing and replacing cards. Ensure that the chassis is electrically connected to earth ground. Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the clip to an unpainted surface of the chassis frame to safely channel unwanted ESD voltages to ground. To properly guard against ESD damage and shocks, the wrist strap and cord must operate effectively. If no wrist strap is available, ground yourself by touching the metal part of the chassis.

Caution For safety, periodically check the resistance value of the antistatic strap, which should be between 1 and 10 megohm (Mohm).

Software Requirements

The MICA carrier card requires the following images:

- Cisco IOS Release 11.3(2)T or later
- Boot Flash image Release 11.2(11)P
- Modem code version 2.2.3.0 (56K)

Caution Before physically installing a MICA carrier card in an Cisco AS5200, you must upgrade the boot Flash image in the access server's boot Flash memory as described in the section "Installing a New MICA Carrier Card."

Required Tools and Equipment

To install the MICA modules and carrier cards, you will need the following tools and equipment which are not included:

- Blank slot covers for open slots
- Medium-size flat-head screwdriver (1/4 in. [0.625 cm])
- ESD-preventive wrist strap and mat
- Antistatic bag (optional)

MICA Carrier Card Indicators

The LEDs on the front panel of the MICA carrier card (see Figure 1) indicate the current operating condition of the 6-port MICA modules installed on the card. You can observe the LEDs, note any fault condition that the product is encountering, and then contact your system administrator or a customer service representative, if necessary. See the section "Cisco Connection Online," for details. Refer to Table 1 for a description of the LEDs.

Figure 1 MICA Carrier Card LEDs

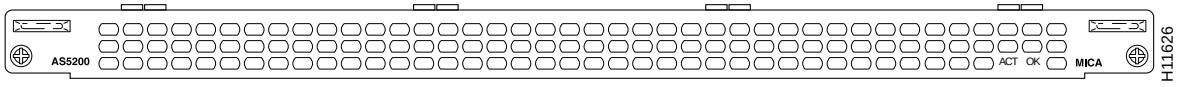


Table 1 MICA Carrier Card LEDs

LED	State	Description
Activity (ACT)[1]	Flickering	There is modem call activity on the MICA modules.
	Off	There is no modem call activity on the MICA modules.
Board OK (OK)	One flash	The carrier card is powering up.

Table 1 MICA Carrier Card LEDs

LED	State	Description
	On	The carrier card has passed initial power-up diagnostics tests and is operating normally.
	Off	A fault condition occurred.

1. The individual 6-port MICA modules do not include LEDs.

Installing a New MICA Carrier Card

Successful installation of the new MICA modem carrier card requires these steps:

1. Upgrade the Cisco IOS image
2. Upgrade the Boot Flash image
3. Install the MICA carrier card
4. Upgrade modem code (optional)

See the following sections for details.

Upgrade the Cisco IOS Image

If you own a SMARTnet contract, you can obtain the Cisco IOS image at Cisco's Software Center home page at the following URL (this is subject to change without notice):

```
http://www.cisco.com/kobayashi/sw-center
```

Upgrade the Boot Flash Image

Before you physically install your new 6-port MICA carrier card, you must upgrade the boot Flash image in the access server boot Flash memory.

Caution Unless you upgrade the image **before** installing the carrier card, the installation will not be successful. Also, if your access server has only 4 MB of boot Flash, Cisco recommends upgrading to 8 MB of boot Flash as you might not have enough room to upgrade to the new boot Flash image. If you do not upgrade the boot Flash and wish to upload the new image to the 4-MB boot Flash, we recommend copying the contents of your boot Flash to a PC hard disk or network server location, and then erasing the boot Flash when prompted by the system. You can follow the procedures in the sections, "Upgrading Modem Code from the Cisco CCO TFTP Server" and "Upgrading Modem Code from Diskettes," later in this configuration note, to grade the boot Flash image.

Install the MICA Carrier Card

Caution Before installing the card, make sure you have upgraded the Cisco IOS image and the boot Flash image, as described in the sections Upgrade the Cisco IOS Image, page 6 and Upgrade the Boot Flash Image, page 6.

Warning Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.

Warning Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages.

Warning Do not work on the system or connect or disconnect cables during periods of lightning activity.

Warning This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.

Warning Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

For DC-powered units only, note the following warning:

Warning Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.

To install a new MICA module carrier card (see Figure 2), do the following:

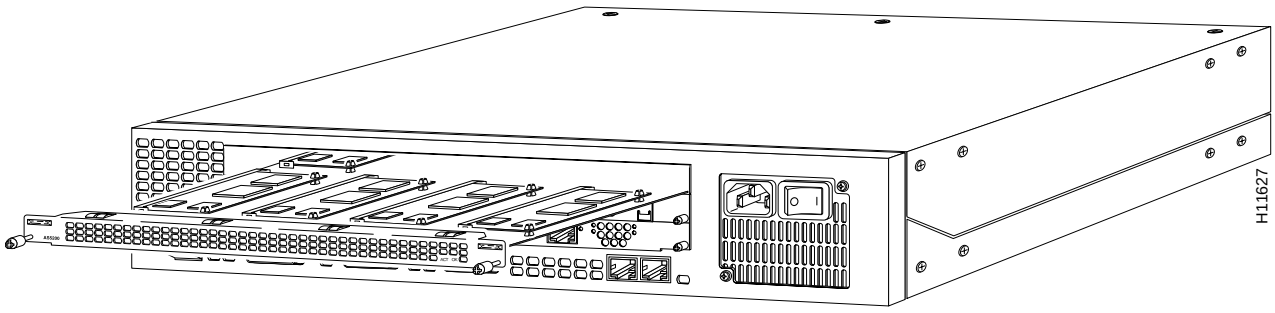
Step 1 Remove the carrier card from the ESD-preventive mat.

Step 2 Slide the carrier card into the slot until it touches the backplane connector.

Step 3 Align the captive screws with their holes, and then seat the carrier card completely.

Step 4 Tighten the two captive screws to secure the carrier card to the chassis.

Figure 2 Carrier Card Installation



Step 5 If the access server is configured with fewer than three cards, ensure proper airflow inside the chassis by installing a blank slot cover is installed over each open slot. Note that you can order blank slot covers from Cisco. The part number is AS52M-BLANK=.

Removing a MICA Carrier Card

Caution The MICA carrier cards are not hot-swappable (that is, you cannot remove or install them when the power to the access server is ON). Be sure to turn OFF the power to the access server before installing or removing carrier cards. *Failure to do so can damage the access server.*

Warning Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.

Warning Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages.

Warning Do not work on the system or connect or disconnect cables during periods of lightning activity.

Warning This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.

Warning Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

For DC-powered units only, note the following warning:

Warning Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.

To remove the MICA carrier card, perform the following steps:

Step 1 Attach an ESD-preventive wrist strap.

Step 2 Power OFF the access server.

Step 3 On the back of the access server, locate the MICA carrier card (see Figure 1).

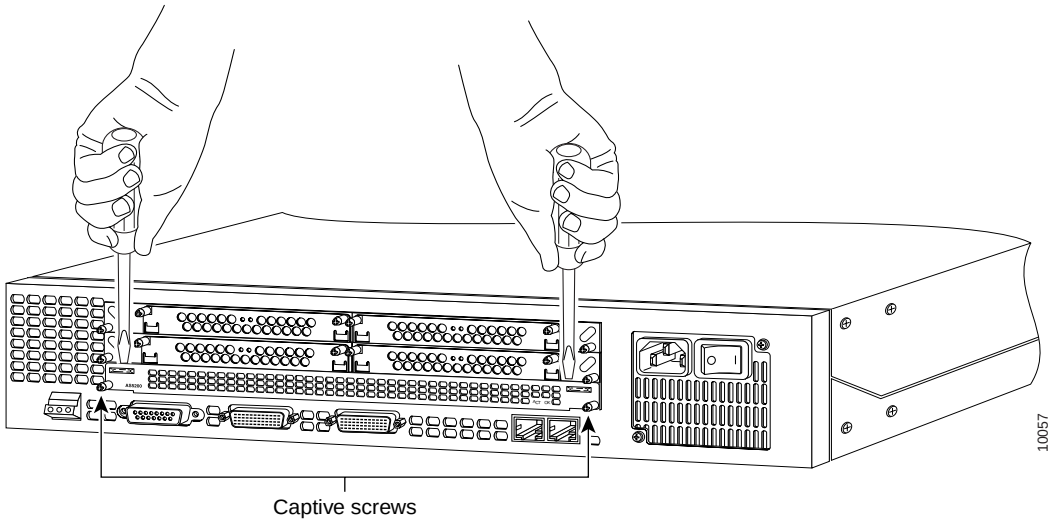
Step 4 Loosen the two captive screws that secure the carrier card to the chassis until each screw is free of the chassis (see Figure 2).

Step 5 Hold the captive screws and gently pull the carrier card free of the chassis. If the card is hard to remove, insert a flat-head screwdriver vertically into the left and right sides of the board and gently pry the board loose (see Figure 3). Then, hold the captive screws and gently pull out the carrier card.

Step 6 Set the removed carrier card aside on an ESD-preventive mat.

Caution The EMI protective devices on the carrier cards are designed to make the cards fit tightly. When removing the cards, they can release suddenly. Exercise caution when removing cards.

Figure 3 Prying the Carrier Card Loose



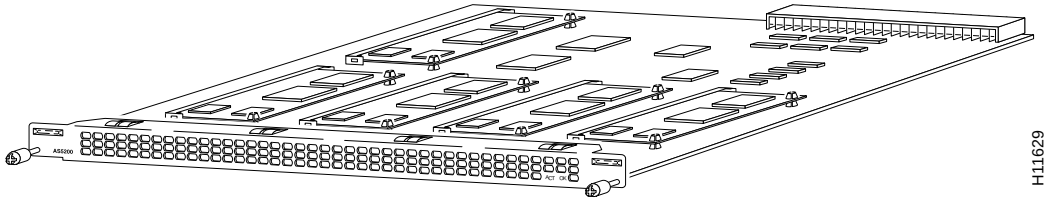
Removing a 6-Port MICA Module

To remove the 6-port MICA modules, perform the following steps:

Step 1 Make sure that you have attached an ESD-preventive wrist strap and that the system is powered OFF.

Step 2 On the carrier card, locate the 6-port MICA module you will replace (see Figure 4).

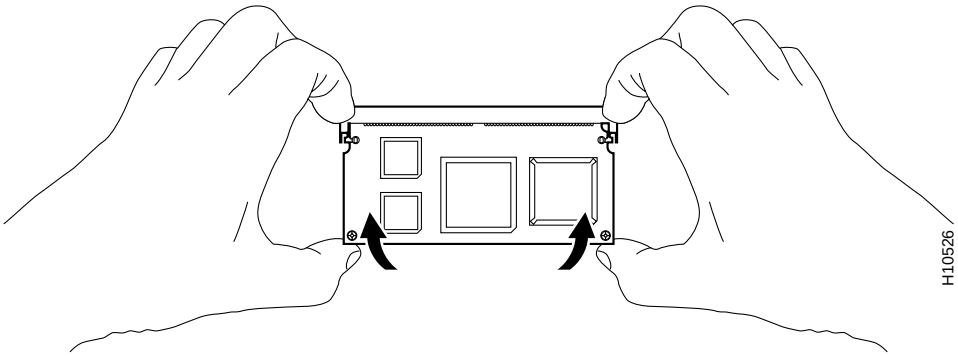
Figure 4 6-Port MICA Carrier Card



Step 3 Orient the module so that the MICA module socket faces away from you.

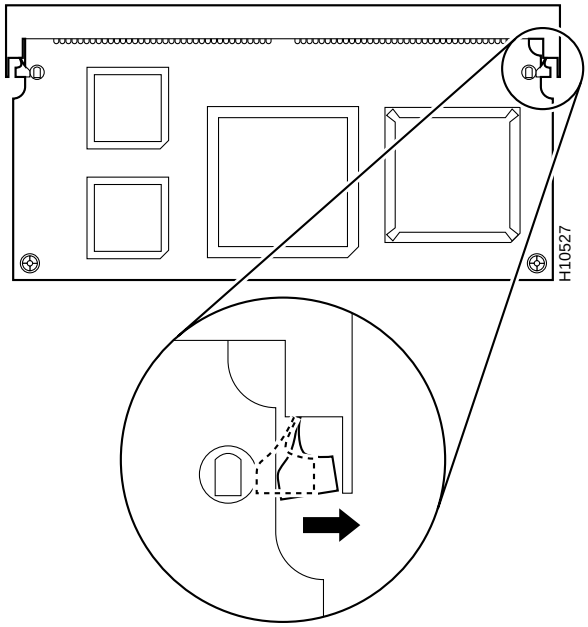
Step 4 Gently pry the edges of the 6-port MICA module away from the standoffs, as shown in Figure 5.

Figure 5 Prying the 6-Port MICA Module from the Standoffs



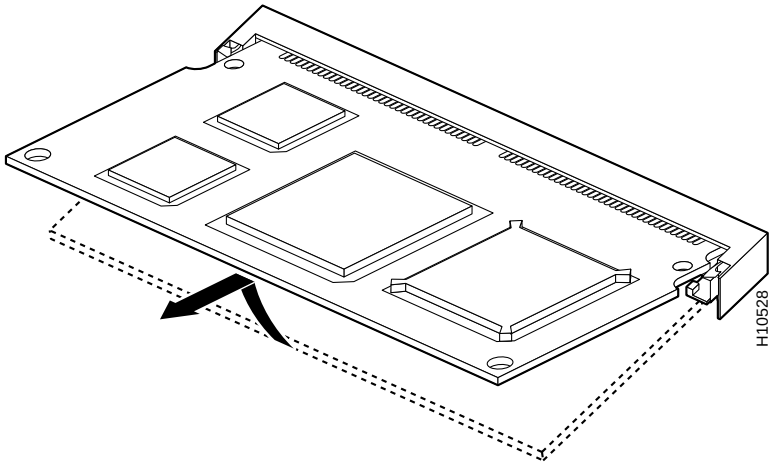
Step 5 Push the two socket latches away from the MICA module, as shown in Figure 6.

Figure 6 Releasing the 6-Port MICA Module from the Socket Latch



Step 6 Remove the MICA module from its socket, as shown in Figure 7.

Figure 7 Removing the 6-Port MICA Module



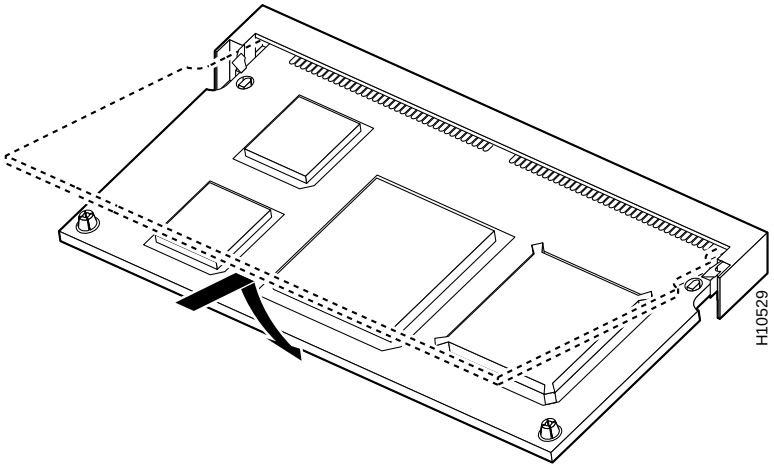
Installing a 6-Port MICA Module

To install a 6-port MICA module:

Step 1 Insert the 6-port MICA module into the socket at a 45° angle.

Step 2 Seat the 6-port MICA module in the socket and press its edges onto the standoffs, as shown in Figure 8.

Figure 8 Installing the 6-Port MICA Module



Upgrading Modem Code

Modem code is a generic term applied to a modem code file, which is also called portware for MICA modems and firmware for Microcom modems.

With new systems, Cisco loads a Cisco IOS software-compatible version of modem code and copies the version to the installed modem modules. A map of the version(s) of modem code copied to the modem RAM for each modem module is stored in nonvolatile random-access memory (NVRAM) so that it is retained over power cycles.

Note You do not have to take any action to use the pre-installed version of modem code with new systems.

You can acquire new modem code in several ways:

- Cisco periodically releases new modem code versions (with bug fixes or new modem features) that improve your system's overall modem performance.
- Cisco also might ship modem code on diskette with spare boards or offer modem code for purchase with spare boards.
- Modem code is also available on the Cisco Software Center (URL http://www.cisco.com/kobayashi/sw-center/) for owners of SMARTnet contracts. Note that this url is subject to change without notice.

This section describes how to upgrade modem code on your access server modems by:

1. Understanding the modem code scenarios possible for your access server.
2. Choosing an upgrade strategy.
3. Finding out the modem code version installed on your access server.
4. Upgrading the modem code.

Caution Cisco ships the access server with the latest version of modem code installed in the boot Flash memory and mapped to the modems. If you choose to use the modem code bundled with your installed Cisco IOS software, you could be reverting to a previous version of modem code. Also note that once you map the bundled modem code (using the **copy system:/ucode/***filename* **modem** or **copy ios-bundled modem** command) to your modems, each time you upgrade the Cisco IOS software, the new bundled modem code is automatically mapped to your modems. See "Displaying Modem Code Versions," later in this document, for details on displaying mode code versions mapped to modems, installed in boot Flash memory, and bundled with the Cisco IOS software on your access server.

How to Obtain Modem Code

You can obtain modem code in one of two ways:

- **Bundled** in regular Cisco IOS releases. See "Using the Modem Code Bundled with Cisco IOS Software" for details.
- **Unbundled** from Cisco Connection Online (CCO) or supplied on diskette. This can be either a more up-to-date version of modem code released before the next Cisco IOS release (when the modem code will be bundled with the Cisco IOS release), or a special version of modem code shipped with a new board. See "Upgrading Modem Code from the Cisco CCO TFTP Server" and "Upgrading Modem Code from Diskettes" for details.

Important Modem Upgrade Commands

There are several commands you use to upgrade modem code. For examples on using the commands, see "Upgrading Modem Code from the Cisco CCO TFTP Server," "Upgrading Modem Code from Diskettes," and "Using the Modem Code Bundled with Cisco IOS Software," later in this document, for details.

- Use the **copy tftp flash** *filename* command to copy any version of modem code (no matter how it is obtained) into boot Flash memory. You can store several versions of the modem code in boot Flash memory under different filenames.
- Use the **copy bootflash modem** command to transfer a specified version (*filename*) of modem code from boot Flash memory to the modem RAM and map that version to the modem modules (slots/ports) specified in response to the modem range query.
- Use the **copy system:/ucode/***filename* **modem** command (or, for Cisco IOS releases earlier than 11.3A or 12.0, the **copy ios-bundled** command) to transfer the version of modem code bundled with Cisco IOS software release to the modem RAM and map that version to the modem modules (slots/ports) specified in response to the modem range query. To view a list of microcode filenames, use the **dir system:/ucode** command.

Choosing an Update Strategy

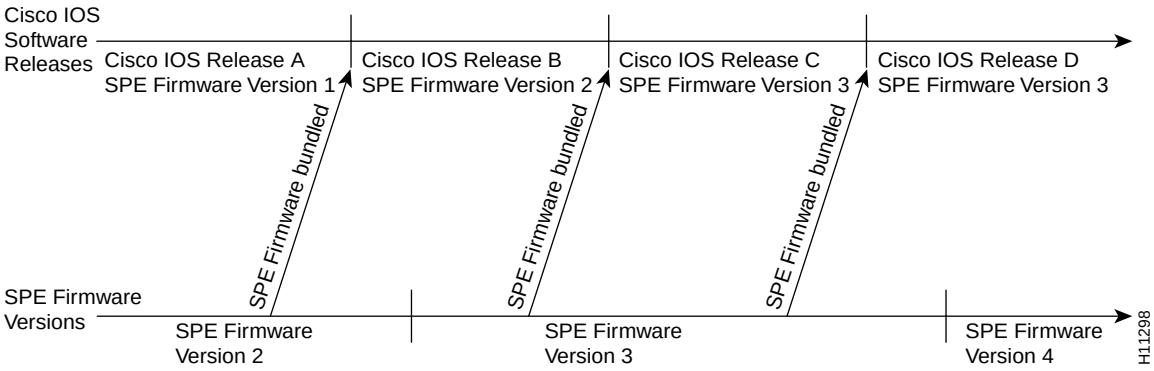
Because of multiple versions of modem code and the way Cisco IOS software processes these versions, Cisco suggests that you choose one of the following two strategies:

- Always allow Cisco IOS software to select the version of modem code.
- Always control the version of modem code used by the modules, independent of Cisco IOS selections.

Caution Cisco ships the access server with the latest version of modem code installed in the boot Flash memory and mapped to the modems. If you choose to use the modem code bundled with your installed Cisco IOS software, you could be reverting to a previous version of modem code. Also note that once you map the bundled modem code (using the **copy system:/ucode/***filename* **modem** or **copy ios-bundled modem** command) to your modems, each time you upgrade the Cisco IOS software, the new bundled modem code is automatically mapped to your modems. See "Displaying Modem Code Versions," later in this document, for details on displaying mode code versions mapped to modems, installed in boot Flash memory, and bundled with the Cisco IOS software on your access server.

To help with the decision, Figure 9 shows a hypothetical release process. Using the modem code bundled with Cisco IOS software is the easier strategy and enables you to take advantage of new modem code whenever you upgrade your Cisco IOS software. Note that you can also control the modem code by reverting to previous versions using the **copy** command as discussed later.

Figure 9 Release Timeline for Cisco IOS Software and Modem Code



Modem Code Scenarios

Table 2 provides scenarios that can occur when you upgrade Cisco IOS software or modem code.

Table 2 Modem Code Scenarios—Cisco IOS Software or Modem Code Upgrades

No.	Scenario	Update Process
1	You receive a new access server from the Cisco factory.	• No action needed. The factory loads and maps a compatible version of modem code.[1]
2	You update Cisco IOS software, and decide to use the version of modem code selected by Cisco IOS software.	• Update Cisco IOS software. • No further action needed—Cisco IOS software automatically downloads either its bundled version or a mapped version from boot Flash memory.[2]
3	You update Cisco IOS software, and decide *not* to use the modem code selected by Cisco IOS software.	• Update Cisco IOS software. • Copy the desired version of modem code file to boot Flash memory, then copy that file to the integrated modems on the 6-port module. See “Copy the Modem Code File from the Local TFTP Server to Modems,” later in this document, for details.
4	The modems are running a version of modem code from boot Flash memory that is different than the version bundled with Cisco IOS software. You decide to revert to the bundled version.	• Use the Cisco IOS command **copy system:/ucode/***filename* **modem** (or, for Cisco IOS releases earlier than 11.3A or 12.0, **copy ios-bundled modem**). Note that once you map the bundled modem code to your modems, each time you upgrade the Cisco IOS software, the new bundled modem code is automatically mapped to your modems. See “Using the Modem Code Bundled with Cisco IOS Software” for details.
5	Cisco releases new modem code, which is a later version than the version currently running on the modems. You decide to use the new Cisco modem code.[3]	• Copy the desired version of modem code file to boot Flash memory, then copy that file to the integrated modems on the 6-port module. See “Copy the Modem Code File from the Local TFTP Server to Modems,” later in this document, for details.

1. To find out the version of modem in your system, use the **show modem mapping** command. This command displays the versions bundled with Cisco IOS software (copied into Flash memory) and running on the modems.
2. In part, Cisco IOS software bases this decision on the last **copy** command issued. For more details about mapping, see Table 4.
3. Cisco might ship this modem code on a diskette packed with the 6-port MICA module.

Figure 10 shows a release timeline and Table 3 explains the resulting versions of Cisco IOS software and modem code.

Figure 10 Release Timeline for Cisco IOS Software and Modem Code

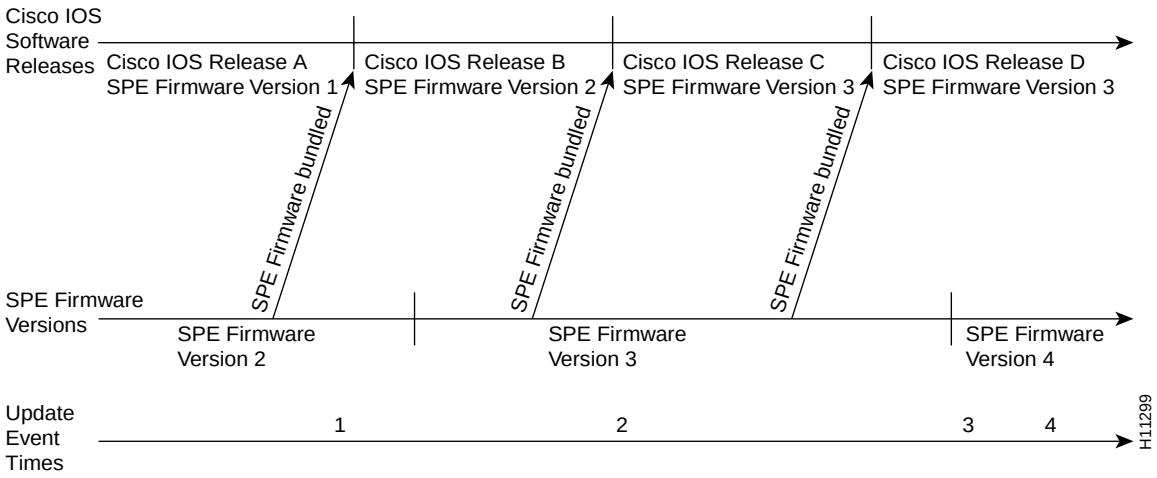


Table 3 Resulting Versions of Cisco IOS Software and Modem Code

Update Event Time	Update Event	Resulting Version of Cisco IOS Software and Modem Code
1	You upgrade Cisco IOS software to Release B.	
	• If there is no previous **copy** command, Cisco IOS software uses the bundled version.	• Cisco IOS Release B Modem Code Version 2
	• If invalid mapping, Cisco IOS software uses the bundled version.	• Cisco IOS Release B Modem Code Version 2
	• If last copy command was **copy system:/ucode/***filename* **modem** (or, for Cisco IOS releases earlier than 11.3A or 12.0, **copy ios-bundled modem**), Cisco IOS software uses the bundled version.	• Cisco IOS Release B Modem Code Version 2
	• If last copy command was **copy bootflash modem** and Modem Code Version 1 was specified, Cisco IOS software copies the modem code from the boot Flash memory to the modems.	• Cisco IOS Release B Modem Code Version 1
2	You upgrade Cisco IOS software to Release C. (Cisco IOS software uses mapping from last **copy** command at Time 1).[1]	Cisco IOS Release C Modem Code Version 1
	You enter the **copy system:/ucode/***filename* **modem** command (or, for Cisco IOS releases earlier than 11.3A or 12.0, the **copy ios-bundled modem** command).	Cisco IOS Release C Modem Code Version 3
3	New Modem Code Version 4 is released, you copy the file to boot Flash memory, enter **copy bootflash modem,** and specify Modem Code Version 4.	Cisco IOS Release C Modem Code Version 4
4	You upgrade Cisco IOS software to Release D.	Cisco IOS Release D Modem Code Version 4
	You enter the **copy system:/ucode/***filename* **modem** command (or, for Cisco IOS releases earlier than 11.3A or 12.0, the **copy ios-bundled modem** command).	Cisco IOS Release D Modem Code Version 3

1. This example assumes the last copy command was **copy bootflash modem**, and Modem Code Version 1 was specified.

Table 4 provides a list of modem code terminology and a description of how the terms are used in the modem code update process.

Table 4 Modem Code Terminology and Commands

Term	Description
Modem Code	Modem code resides in and runs out of modem RAM. Cisco IOS software transfers a version of modem code to modem RAM on each reboot and reload. Boot Flash memory can contain several versions of modem code: a version bundled with Cisco IOS software and multiple versions that resulted from previous **copy tftp bootflash** commands.
copy system:/ucode/*filename* **modem** command (or, for Cisco IOS releases earlier than 11.3A or 12.0, **copy ios-bundled** command	This command transfers the version of modem code bundled with Cisco IOS software to the modem RAM and maps that version to the modem modules specified by the modem range. This command does not affect any existing versions of modem code that reside in boot Flash memory. After one such command, future Cisco IOS upgrades will potentially result in the downloading of new Cisco IOS software bundled firmware to the modems. (If the new Cisco IOS image contains the same modem code as the old one, no new code will be downloaded to the modems.)
copy tftp bootflash *filename* command	Places a copy of the modem code in boot Flash memory.
copy bootflash modem command	This command transfers the version of modem code in boot Flash memory to the modem RAM and maps that version to the modem modules specified by the modem range.
Mapping commands	The copy commands map a specific version of modem code to a group of modem slots/ports. The **copy system:/ucode/***filename* **modem** (or **copy ios-bundled modem**) command maps the slots/ports to the bundled version, and the **copy bootflash modem** command maps the slots/ports to the boot Flash memory version. Cisco IOS software uses the mapping to determine which version of modem code should be downloaded to the modems. If Cisco IOS software finds no mapping or invalid mapping, it downloads the bundled version. Although modem ranges are specified as slot/port, the modem code is downloaded on a per module basis. The **show modem mapping** command lists all Cisco IOS software and modem code files (bundled and unbundled) and their versions in the boot Flash memory and system Flash memory. This will help you decide if you need to update your modem code files.[1]

1. This command is supported in Cisco IOS Releases 11.2(11)P and 11.3(2)T.

Displaying Modem Code Versions

Use the **show modem mapping** command to list all modem code files in the boot Flash memory, system Flash memory, and the modem code files bundled with Cisco IOS software. This will help you decide if you need to update your modem code files.

```
5200# show modem mapping

Slot 1 has Mica Carrier card.


        Modem      Firmware   Firmware
```

```
Module  Numbers    Rev        Filename
  0   1/0  - 1/5   2.2.3.0    bootflash:mica-modem-portware.2.2.3.0.bin
  1   1/6  - 1/11  2.2.3.0    mica-modem-portware.2.2.3.0.bin
  2   1/12 - 1/17  2.2.3.0    mica-modem-portware.2.2.3.0.bin
  3   1/18 - 1/23  2.2.3.0    mica-modem-portware.2.2.3.0.bin
  4   1/24 - 1/29  2.2.3.0    mica-modem-portware.2.2.3.0.bin

Slot 2 has Mica Carrier card.


        Modem      Firmware   Firmware
Module  Numbers    Rev        Filename
  0   2/0  - 2/5   2.2.3.0    flash:1:mica-modem-portware.2.2.3.0.bin
  1   2/6  - 2/11  2.2.3.0    mica-modem-portware.2.2.3.0.bin
  2   2/12 - 2/17  2.2.3.0    mica-modem-portware.2.2.3.0.bin
  4   2/24 - 2/29  2.2.3.0    mica-modem-portware.2.2.3.0.bin

IOS Bundled Firmware Information:

Mica Boardware Version : 1.0.0.0
Mica Portware Version : 2.2.30


Firmware files on Boot Flash:

Firmware-file                              Version  Firmware-Type
=============                              =======  =============
bootflash:mica-modem-portware.2.2.3.0.bin  2.2.3.0  Mica Portware
```

Upgrading Modem Code from the Cisco CCO TFTP Server

Note You can access the Cisco CCO TFTP server only if you own a SMARTnet contract.

Upgrading modem code from the Cisco CCO TFTP server is a two-step process:

- Download Modem Code from the Cisco CCO TFTP Server to a Local TFTP Server
- Copy the Modem Code File from the Local TFTP Server to Modems

Download Modem Code from the Cisco CCO TFTP Server to a Local TFTP Server

You can download software from the CCO TFTP server using an Internet browser or FTP application. Both procedures are described below.

Note To download modem code from CCO to a PC and then upgrade the modem code to an access server connected to your PC via an Ethernet hub, you need to set up a TFTP application on your PC, establish a HyperTerminal session, and make sure your PC and access server are correctly connected and talking before downloading the modem code from CCO. All these procedures are described in "Upgrading Modem Code from Diskettes," later in this document.

Using an Internet Browser

Step 1 Launch an Internet browser.

Step 2 Bring up the Cisco Software Center home page at the following URL (this is subject to change without notice):

http://www.cisco.com/kobayashi/sw-center/

Step 3 Click **Access Products** (under **Cisco Software Products**) to open the **Access Products** window.

Step 4 Click **Cisco AS5200 Series Software**.

Step 5 Click the modem code you want and download it to your workstation or PC.

Step 6 Click the modem code file you want to download, and then follow the remaining download instructions. If you are downloading the modem code file to a PC, make sure you download it to the c:\tftpboot directory; otherwise, the download process will not work.

Step 7 When the modem code is downloaded to your workstation, transfer the file to a TFTP server in your LAN using a terminal emulation software application.

Using an FTP Application

Note The directory path leading to the modem code files on cco.cisco.com is subject to change without notice. If you cannot access the files using an FTP application, try the Cisco Software Center URL http://www.cisco.com/kobayashi/sw-center/.

Step 1 Log in to Cisco CCO FTP server called cco.cisco.com:

```
terminal> ftp cco.cisco.com
Connected to cio-sys.cisco.com.
220-
220-  Cisco Connection Online       |        |      Cisco Systems, Inc.
220-  Email: cco-team@cisco.com   |||      |||  170 West Tasman Drive
220-  Phone: +1.800.553.2447  .:|||||:..:|||||:.  San Jose, CA 95134
220-
220-
220-  NOTE: As of February 1,1997 ftp.cisco.com will now point to this
220-  service. Please be advised. To use the former ftp.cisco.com after
220-  February 1, connect to ftpeng.cisco.com
220-
220-  You may login with:
220- + Your CCO username and password, or
220- + A special access code followed by your e-mail address, or
220- + "anonymous" followed by your e-mail address for guest access.
220-
220 cio-sys FTP server (CIOESD #103 Sun Dec 15 14:43:43 PST 1996) ready.
```

Step 2 Enter your CCO registered username and password (for example, **harry** and **letmein**):

```
Name (cco.cisco.com:harry): harry
331 Password required for harry.
Password: letmein
230-############################################################
230-#  Welcome to the Cisco Systems CCO FTP server.
230-#  This server has a number of restrictions.  If you are not familiar
230-#  with these, please first get and read the /README or /README.TXT file.
230-#  http://www.cisco.com/acs/info/cioesd.html for more info.
230-############################################################
```

```
230-
230-  *****  NOTE: As of February 1, 1997, "cco.cisco.com",   *****
230-  *****  "www.cisco.com" and "ftp.cisco.com" are now all  *****
230-  *****  logical names for the same machine.              *****
230-  *****                                                   *****
230-  *****  The old "ftp.cisco.com" is an entirely          *****
230-  *****  different machine, which is now known as        *****
230-  *****  "ftpeng.cisco.com" or "ftp-eng.cisco.com".      *****
230-  *****                                                   *****
230-  *****  In general, "ftpeng.cisco.com" is used only for  *****
230-  *****  distribution of Cisco Engineering-controlled     *****
230-  *****  projects, such as beta programs, early field     *****
230-  *****  trials, developing standards documents, etc.     *****
230-  *****                                                   *****
230-  *****  Be sure to confirm you have connected to         *****
230-  *****  the machine you need to interact with.           *****
230-
230-  If you have any odd problems, try logging in with a minus sign (-) as
230-  the first character of your password.  This will turn off a feature
230-  that may be confusing your ftp client program.
230-  Please send any questions, comments, or problem reports about this
230-  server to cco-team@cisco.com.
230-
230-  NOTE:
230-  o To download files from CCO, you must be running a *passive-mode*
230-    capable FTP client.
230-  o To drop files on this system, you must cd to the /drop directory.
230-  o Mirrors of this server can be found at
230-
230-     + ftp://www-europe.cisco.com European (Amsterdam)
230-     + ftp://www-fr.cisco.com     France     (Paris)
230-     + ftp://www-au.cisco.com     Australia  (Sydney)
230-     + ftp://www-jp.cisco.com     Japan      (Tokyo)
230-     + ftp://www-kr.cisco.com     Korea      (Seoul)
230-
230-Please read the file README
230-  it was last modified on Sat Feb  1 12:49:31 1997 - 163 days ago
230 User harry logged in.  Access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Step 3 Specify the directory path that holds the modem modem code you want to download. For example, the directory path for the Cisco AS5200 modem code is /cisco/access/5200:

```
ftp> cd /cisco/access/5200
250-Please read the file README
250-  it was last modified on Tue May 27 10:07:38 1997 - 48 days ago
250-Please read the file README.txt
250-  it was last modified on Tue May 27 10:07:38 1997 - 48 days ago
250 CWD command successful.
```

Step 4 View the contents of the directory with the **ls** command:

```
ftp> ls
227 Entering Passive Mode (192,31,7,130,218,128)
150 Opening ASCII mode data connection for /bin/ls.
total 2688
drwxr-s--T   2 ftpadmin ftpcio    512 Jun 30 18:11 .
drwxr-sr-t  19 ftpadmin ftpcio    512 Jun 23 10:26 ..
lrwxrwxrwx  1  root     3          10 Aug   6 1996     README ->README.txt
-rw-rw-r--   1 root     ftpcio   2304 May 27 10:07 README.txt
-r--r--r-- 1 ftpadmin ftpint 377112 Jul 10 18:08
images/mica-modem-portware.2.2.3.0.bin
-r--r--r-- 1 ftpadmin ftpint 635 Jul 10 18:08 images/mica-modem-portware.readme
226 Transfer complete.
```

Step 5 Specify a binary image transfer:

```
ftp> binary
200 Type set to I.
```

Step 6 Copy the modem code files from the Cisco AS5200 to your local environment with the **get** command.

```
ftp> get images/mica-modem-portware.2.2.3.0.bin
PORT command successful.
Opening BINARY mode data connection for images/mica-modem-portware.2.2.3.0.bin
(280208 bytes).
Transfer complete.
local: images/mica-modem-portware.2.2.3.0.bin
remote: images/mica-modem-portware.2.2.3.0.bin
385503 bytes received in 3.6 seconds (1e+02 Kbytes/s)
```

Step 7 Quit your terminal session:

```
ftp> quit
Goodbye.
```

Step 8 Verify you successfully transferred the files to your local directory:

```
5200% ls -al
total 596
-r--r--r-- 1 280208 Jul 10 18:08 images/mica-modem-portware.2.2.3.0.bin
5200% pwd
/auto/tftpboot
```

Step 9 Transfer these files to a local TFTP or RCP server that your access server can access.

Copy the Modem Code File from the Local TFTP Server to Modems

The procedure for copying the modem code file from your local TFTP server to the modems involves two steps. First, you need to transfer the code to the access server's boot Flash memory. Then, you need to transfer the code to the modems.

These two steps are performed only once. After you copy the modem code file into boot Flash memory for the first time, you should not have to perform these steps again. Because the modem code runs from modem RAM, the Cisco IOS software automatically copies the modem code to each modem each time the access server power cycles.

Perform the following steps to download modem code to MICA modems:

Step 1 Establish an xterm session to the access server if using a UNIX workstation, or a HyperTerminal session to the access server if using a PC. For details on establishing a HyperTerminal session, see "Upgrading Modem Code from Diskettes," later in this document, for details.

Step 2 Enter the access server enable mode (the prompt is displayed as `5200#`):

```
5200> enable
Password: <password>
5200#
```

Step 3 Check the files in the access server boot Flash memory:

```
5200# show bootflash
Boot flash directory:
File  Length   Name/status
  1   3405148  c5200-boot-l
[3405148 bytes used, 4983460 available, 8388608 total]
8192K bytes of processor board Boot flash (Read/Write)
```

Step 4 Download the modem code file from TFTP server into the access server boot Flash memory using the **copy tftp bootflash** command. After you enter the command, you are prompted for the download destination and the remote host name as requested by the system software.

```
5200# copy tftp bootflash

Boot flash directory:
File  Length   Name/status
  1   3405148  c5200-boot-l
[3405212 bytes used, 4983396 available, 8388608 total]
Address or name of remote host [jurai]? jurai
Source file name? mica-modem-portware.2.2.3.0.bin
Destination file name [mica-modem-portware.2.2.3.0.bin]?
mica-modem-portware.2.2.3.0.bin
Accessing file 'mica-modem-portware.2.2.3.0.bin' on jurai...
Loading mica-modem-portware.2.2.3.0.bin from 223.255.254.254 (via Ethernet0): !
[OK]

Erase flash device before writing? [confirm] no
Copy file? [confirm] yes

Copy 'mica-modem-portware.2.2.3.0.bin' from 5200
  as 'mica-modem-portware.2.2.3.0.bin' into Flash WITHOUT erase? [yes/no] yes
Loading mica-modem-portware.2.2.3.0.bin from 223.255.254.254 (via Ethernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 209118/4983396 bytes]

Verifying checksum...  OK (0xBFC6)
Flash device copy took 00:00:07 [hh:mm:ss]
5200#
```

Step 5 Verify the file has been copied into the access server boot Flash memory:

```
5200# show bootflash

Boot flash directory:
File  Length   Name/status
  1   3405148  c5200-boot-l
  2   209118   mica-modem-portware.2.2.3.0.bin
  3   371202   mcom-modem-code-3.2.10.bin
[3985468 bytes used, 4403140 available, 8388608 total]
8192K bytes of processor board Boot flash (Read/Write)
```

Step 6 Copy the modem code file from the access server boot Flash memory to the modems by entering the **copy bootflash modem** command:

```
5200# copy bootflash modem
Modem Numbers (<slot>/<port> | group <number> | all)? all

Boot flash directory:
File  Length   Name/status
  1   3405148  c5200-boot-l
  2   209118   mica-modem-portware.2.2.3.0.bin
  3   371202   mcom-modem-code-3.2.10.bin
[3985468 bytes used, 4403140 available, 8388608 total]
Name of file to copy?  mica-modem-portware.2.2.3.0.bin

Type of service [busyout/reboot] busyout
Copy 'bootflash:mica-modem-portware.2.2.3.0.bin' from Bootflash to modems?
[yes/no] yes

5200#
```

```
*Mar  1 00:10:03.159: %MODEM-5-DL_START: Modem (1/0) started firmware download
*Mar  1 00:10:03.159: %MODEM-5-DL_START: Modem (1/1) started firmware download
*Mar  1 00:10:03.163: %MODEM-5-DL_START: Modem (1/2) started firmware download
.
.
.
*Mar  1 00:10:13.823: %MODEM-5-DL_GOOD: Modem (1/2) completed firmware download:
*Mar  1 00:10:13.823: %MODEM-5-DL_GOOD: Modem (1/3) completed firmware download:
*Mar  1 00:10:13.827: %MODEM-5-DL_GOOD: Modem (1/4) completed firmware download:
*Mar  1 00:10:13.831: %MODEM-5-DL_GOOD: Modem (1/5) completed firmware download:
```

Note The modem code is downloaded to the module, not the individual slot/ports as indicated by the screen display.

Upgrading Modem Code from Diskettes

This section describes how to copy modem code from diskettes to your hard disk in a PC environment, and then upload the modem code to the modems. The steps are similar if you are using a Macintosh or UNIX workstation.

Note If you loaded Cisco IOS software from a feature pack CD-ROM using Router Software Loader (RSL), note that the CD contains a TFTP server program for PCs using Microsoft Windows 95. Run the TFTP server program from the directory where you installed the RSL program. Remember to set the root directory to the directory where the Cisco AS5200 modem code is located. The RSL and the TFTP applications are also available on CCO in the software library in the Access Products section.

Copy the Modem Code to Your PC Hard Disk

This section describes how to copy the modem code file to your hard disk in a PC environment. The steps are similar if you are using a Macintosh or a UNIX workstation.

Step 1 Insert the modem code diskette in the diskette drive.

Step 2 Use Microsoft Windows 95 Explorer to create a folder named tftpboot at your hard disk root c:.

Step 3 Use the Microsoft Windows 95 Explorer to copy the modem code file into the c:/tftpboot folder.

Copy the Modem Code from Your PC to the Modems

If you are using a PC running Microsoft Windows 95, installing the modem code from a hard drive onto a Cisco AS5200 involves installing a TFTP application on your PC, connecting your PC and the access server, establishing a HyperTerminal session on your PC, pinging the PC and access server to make sure they are talking to each other, copying the modem code from the PC to the access server, and then mapping the modem code to the modems. See the following sections for details.

Note The steps are similar if you are using a Macintosh or a UNIX workstation.

Set up a TFTP Application on the PC

Step 1 Install the TFTP application on the PC.

Note You can use any TFTP or RCP application available from independent software vendors. A number of TFTP programs are also available as shareware from public sources on the World Wide Web. If you are using Microsoft Windows 95, you can also download a TFTP application (as zipped files) from the Cisco Software Center at the URL http://www.cisco.com/kobayashi/sw-center/.

Step 2 Launch the TFTP application by double-clicking the application icon or its filename.

Step 3 Set your TFTP server root directory:

- Choose **Server Root Directory** from the Options menu.
- Choose **c:\tftpboot** from the **Drives** and **[...]** list boxes.
- Click **OK**.

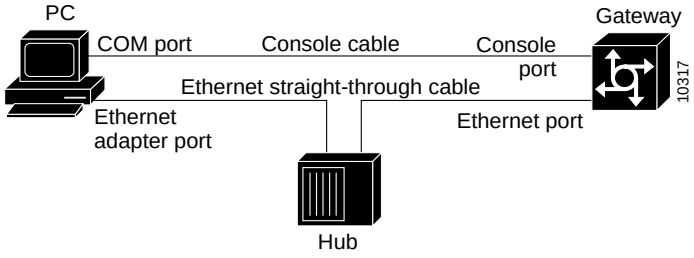
Caution If you do not select the c:\tftpboot directory as your TFTP server directory, you will not be able to perform the copy procedure. This also applies if you are using RCP on your system.

Connect Your PC and the Access Server

In this step, you connect your PC and access server.

Step 1 Use straight-through cables to connect the PC and access via a 10BaseT hub, as shown in Figure 11. Also note that both Ethernet ports must have the same baseband.

Figure 11 Connecting a PC and the Access Server



Note You can also connect your PC Ethernet port directly to the Cisco AS5200 Ethernet port using the 10BaseT crossover cable provided.

Step 2 Connect your PC COM port to the Cisco AS5200 console port, as shown in Figure 11.

Step 3 Make sure your PC and access server are powered on.

Establish a HyperTerminal Session

Use the steps in this section to establish a HyperTerminal session from your local PC to the Cisco AS5200. You will use the HyperTerminal session to talk to the access server.

Step 1 In Microsoft Windows 95 on your PC, choose **Start/Programs/Accessories/HyperTerminal**.

Step 2 Double-click **Hypertrm.exe** to display the Connection Description dialog box.

Step 3 Enter a name for your connection (for example, **Console**) and click **OK**. HyperTerminal displays the Phone number dialog box.

Step 4 Choose the COM port connecting the PC and the access server in the Connect using list box. You have options to connect directly to one of four COM ports.

Step 5 Click **OK**. HyperTerminal displays the COM Properties dialog box.

Step 6 Choose these options in the COM Properties dialog box:

- Bits per second: **9600**
- Data bits: **8**
- Parity: **None**
- Stop bits: **1**
- Flow control: **None**

Step 7 Click **OK**. The HyperTerminal dialog box appears.

Step 8 Press **Enter** to display the `5200#` prompt.

Note If the access server prompt does not appear, you might have selected the wrong COM port, the cable connections could be incorrect or bad, or the access server might not be powered on.

Ping the PC and Access Server

Ping the access server and the PC to make sure they are talking to each other and there are no configuration problems on your access server.

Step 1 Choose the correct Ethernet adapter connecting to the access server and note the PC IP address:

(a) Choose **Start/Run** to display the Run dialog box.

(b) Enter **winipcfg** and click **OK** to display the IP Configuration dialog box.

(c) Choose the PC Ethernet adapter connector used for the connection to the access server if you have more than one Ethernet adapter connector installed on your PC.

(d) Make a note of the PC IP address, and then click **OK**.

Note Enter the **show running config** command at the `5200#` prompt to verify the access server has an IP address assigned. If the access server does not have an IP address, assign an IP address before continuing.

Step 2 In the HyperTerminal dialog box (see the previous section "Establish a HyperTerminal Session" for details), enter the access server enable mode (the prompt is displayed as 5200#):

```
5200> enable
Password: <password>
5200#
```

Step 3 Enter the **ping** command with your PC IP address:

```
5200# ping 131.108.1.1
```

The access server displays five exclamation points (!) if everything is working and it displays five dots (.) if there is a problem. In the latter case, check the cabling between the router and the PC and check the access server configuration.

Upload Modem Code to the Access Server

The procedure for copying the modem code file from your PC set up as a local TFTP server to the access server boot Flash memory is a two-step process.

- Transfer the code to the access server.
- Transfer the code to the modems.

These two steps are performed only once. After you copy the modem code file into boot Flash memory for the first time, you should not have to perform these steps again. Because the modem code runs from modem RAM, the Cisco IOS software automatically copies the code to each modem each time the access server power cycles.

Step 1 Check the modem code version in the access server boot Flash memory:

```
5200# show bootflash

Boot flash directory:
File  Length   Name/status
  1   3405148  c5200-boot-l
[3405148 bytes used, 4983460 available, 8388608 total]
8192K bytes of processor board Boot flash (Read/Write)
```

Step 2 Download the modem code file from the TFTP server into the access server boot Flash memory using the **copy tftp bootflash** command. After you enter the command, you are prompted for the download destination and the remote host name as requested by the system software.

```
5200# copy tftp bootflash

Boot flash directory:
File  Length   Name/status
  1   3405148  c5200-boot-l
[3405212 bytes used, 4983396 available, 8388608 total]
Address or name of remote host [jurai]? jurai
Source file name? mica-modem-portware.2.2.3.0.bin
Destination file name [mica-modem-portware.2.2.3.0.bin]?
mica-modem-portware.2.2.3.0.bin
Accessing file 'mica-modem-portware.2.2.3.0.bin' on jurai...
Loading mica-modem-portware.2.2.3.0.bin from 223.255.254.254 (via Ethernet0): !
[OK]

Erase flash device before writing? [confirm] no
Copy file? [confirm] yes

Copy 'mica-modem-portware.2.2.3.0.bin' from 5200
  as 'mica-modem-portware.2.2.3.0.bin' into Flash WITHOUT erase? [yes/no] yes
```

```
Loading mica-modem-portware.2.2.3.0.bin from 223.255.254.254 (via Ethernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 209118/4983396 bytes]

Verifying checksum...  OK (0xBFC6)
Flash device copy took 00:00:07 [hh:mm:ss]
5200#
```

Step 3 Verify the modem code file has been copied into the access server boot Flash memory:

```
5200# show bootflash

Boot flash directory:
File  Length   Name/status
  1   3405148  c5200-boot-l
  2   209118   mica-modem-portware.2.2.3.0.bin
  3   371202   mcom-modem-code-3.2.10.bin
[3985468 bytes used, 4403140 available, 8388608 total]
8192K bytes of processor board Boot flash (Read/Write)
```

Step 4 Copy the modem code file from the access server boot Flash memory to the modems by entering the **copy bootflash modem** command:

```
5200# copy bootflash modem
Modem Numbers (<slot>/<port> | group <number> | all)? all

Boot flash directory:
File  Length   Name/status
  1   3405148  c5200-boot-l
  2   209118   mica-modem-portware.2.2.3.0.bin
  3   371202   mcom-modem-code-3.2.10.bin
[3985468 bytes used, 4403140 available, 8388608 total]
Name of file to copy?  mica-modem-portware.2.2.3.0.bin

Type of service [busyout/reboot] busyout
Copy 'bootflash:mica-modem-portware.2.2.3.0.bin' from Bootflash to modems?
[yes/no] yes

5200#

*Mar  1 00:10:03.159: %MODEM-5-DL_START: Modem (1/0) started firmware download
*Mar  1 00:10:03.159: %MODEM-5-DL_START: Modem (1/1) started firmware download
*Mar  1 00:10:03.163: %MODEM-5-DL_START: Modem (1/2) started firmware download
.
.
.
*Mar  1 00:10:13.823: %MODEM-5-DL_GOOD: Modem (1/2) completed firmware download:
*Mar  1 00:10:13.823: %MODEM-5-DL_GOOD: Modem (1/3) completed firmware download:
*Mar  1 00:10:13.827: %MODEM-5-DL_GOOD: Modem (1/4) completed firmware download:
*Mar  1 00:10:13.831: %MODEM-5-DL_GOOD: Modem (1/5) completed firmware download:
```

Note The modem code is downloaded to the module, not the individual slot/ports as indicated by the screen display.

Using the Modem Code Bundled with Cisco IOS Software

Use this procedure to update modem code on the modems in your access server if you decide to use the version of modem code bundled with Cisco IOS software instead of the version already mapped to your modems.

Caution Cisco ships the access server with the latest version of modem code installed in the boot Flash memory and mapped to the modems. If you choose to use the modem code bundled with your installed Cisco IOS software, you could be reverting to a previous version of modem code. Also note that after you map the bundled modem code (using the **copy system:/ucode/***filename* **modem** or **copy ios-bundled modem** command) to your modems, each time you upgrade the Cisco IOS software, the new bundled modem code is automatically mapped to your modems. See "Displaying Modem Code Versions," earlier in this document, for details on displaying mode code versions mapped to modems, installed in boot Flash memory, and bundled with the Cisco IOS software on your access server.

To set the modem code mapping to the modem code version bundled with Cisco IOS software, enter the following commands.

Step 1 Enter the access server enable mode (the prompt is displayed as `5200#`):

```
5200> enable
Password: <password>
5200#
```

Step 2 Enter the **copy system:/ucode/***filename* **modem** command (or, for Cisco IOS releases earlier than 11.2A or 12.0, the **copy ios-bundled modem** command):

```
5200# copy ios-bundled modem
Modem Numbers (<slot/<port | group <number | all)? all
Type of service [busyout/reboot] busyout
Copy bundled firmware from IOS image to modems? [yes/no] yes

5200#
*Dec  1 00:12:02.835: %MODEM-5-DL_START: Modem (1/6) started firmware download
*Dec  1 00:12:02.839: %MODEM-5-DL_START: Modem (1/7) started firmware download
*Dec  1 00:12:02.839: %MODEM-5-DL_START: Modem (1/8) started firmware download
*Dec  1 00:12:02.843: %MODEM-5-DL_START: Modem (1/9) started firmware download
*Dec  1 00:12:02.843: %MODEM-5-DL_START: Modem (1/10) started firmware download
*Dec  1 00:12:02.847: %MODEM-5-DL_START: Modem (1/11) started firmware download
*Dec  1 00:12:13.643: %MODEM-5-DL_GOOD: Modem (1/6) completed firmware
 download:
*Dec  1 00:12:13.647: %MODEM-5-DL_GOOD: Modem (1/7) completed firmware
 download:
*Dec  1 00:12:13.651: %MODEM-5-DL_GOOD: Modem (1/8) completed firmware
 download:
*Dec  1 00:12:13.651: %MODEM-5-DL_GOOD: Modem (1/9) completed firmware
 download:
*Dec  1 00:12:13.655: %MODEM-5-DL_GOOD: Modem (1/10) completed firmware
 download:
*Dec  1 00:12:13.659: %MODEM-5-DL_GOOD: Modem (1/11) completed firmware
 download:
```

The **copy system:/ucode/***filename* **modem** (or **copy ios-bundled modem**) command does not affect any existing modem code in boot Flash memory in case you later want to revert to it. If you decide to delete the code from boot Flash memory, remember that *all* files in boot Flash memory will be deleted, therefore save and restore any important files (for example, the Cisco IOS software image).

Note If the new Cisco IOS image contains the same modem code as the old one, no new code will be downloaded to the modems.

Configuring 6-Port MICA Modules

How to Find Command Options

This section explains how to display options for a command. To display options for a command, enter a **?** at the configuration prompt or after entering part of a command followed by a space. The configuration parser displays options available with the command. For example, if you were in global configuration mode, typed the command **arap**, and wanted to see all the keywords and arguments for that command, you would type **arap ?**.

Table 5 shows examples of this function.

Table 5 How to Find Command Options

Command	Comment

`5200>` **enable**
`Password: <`***password***`>`
`5200#`
	Enter enable mode.
	Enter the password.
	You have entered enable mode when the prompt changes to `5200#`.

`5200#` **config terminal**
`Enter configuration commands, one per line. End with CNTL/Z.`
`5200(config)#`
	Enter global configuration mode (the prompt changes to `5200(config)#`).

`5200(config)#` **controller t1 ?** `• <0-1>  Controller unit number` `5200(config)#` **controller t1 1**	Specify the T1 controller that you want to configure using the **controller T1** number global configuration command

`5200(config-controller)#` **?**
`Controller configuration commands:`
`  cablelength  Specify the cable length for a DS1 link`
`  cas-group  Configure the specified timeslots for CAS(Channel Associate Signals)`
`  channel-group  Specify the timeslots to channel-group mapping for an interface`
`  clock  Specify the clock source for a DS1 link`
`  default  Set a command to its defaults`
`  description  Controller specific description`
`  ds0  ds0 commands`
`  exit  Exit from controller configuration mode`
`  fdl  Specify the FDL standard for a DS1 data link`
`  framing  Specify the type of Framing on a DS1 link`
`  help  Description of the interactive help system`
`  linecode  Specify the line encoding method for a DS1 link`
`  loopback  Put the entire T1 line into loopback`
`  no  Negate a command or set its defaults`
`  pri-group  Configure the specified timeslots for PRI`
`  shutdown  Shut down a DS1 link (send Blue Alarm)`
	Display controller configuration commands.

Table 5 How to Find Command Options (Continued)

Command	Comment
5200(config-controller)# **cas-group ?** `<0-23>  Channel number`	Display the options for the cas-group controller configuration command. This command is used to configures the channel-associated signaling on an T1 controller.
5200(config-controller)# **cas-group 1 ?** `timeslots  List of timeslots in the cas-group`	Display the only command (**timeslots**) available in **cas-group 1**.
5200(config-controller)# **cas-group 1 timeslots ?** `<1-24>  List of timeslots which comprise the cas-group`	Display the range for the timeslot option. Specifies a timeslot range of values from 1 to 24. You can specify timeslot ranges (for example, 1-24), individual timeslots separated by commas (for example 1, 3, 5), or a combination of the two (for example 1-3, 8, 17-24). The 16th time slot is not specified in the command line, because it is reserved for transmitting the channel signaling.

5200(config-controller)# **cas-group 1 timeslots 1-24 ?**
`service  Specify the type of service`
`type  Specify the type of signaling`
	Display the two commands (**service** and **type**) available for the timeslots.

5200(config-controller)# **cas-group 1 timeslots 1-24 type ?**
`e&m-fgb  E & M Type II FGB`
`e&m-fgd  E & M Type II FGD`
`e&m-immediate-start  E & M Immediate Start`
`fxs-ground-start  FXS Ground Start`
`fxs-loop-start  FXS Loop Start`
`sas-ground-start  SAS Ground Start`
`sas-loop-start  SAS Loop Start`
	List supported signaling types.

5200(config-controller)# **cas-group 1 timeslots 1-24 type e&m-fgb ?**
`dtmf  DTMF tone signaling`
`mf  MF tone signaling`
`service  Specify the type of service`
`<cr>`
	Display the types of channel-associated signaling available for the e&m-fgb type.

5200(config-controller)# **cas-group 1 timeslots 1-24 type e&m-fgb dtmf ?**
`dnis  DNIS addr info provisioned`
`service  Specify the type of service`
`<cr>`
	Display the options supported for the DTMF tone signaling option.

If you need further assistance, refer to the sections “Cisco Connection Online” and “CD-ROM/WWW Feedback,” later in this document, for more information.

Configure 6-Port MICA Modules

Take the following steps to configure the 6-port MICA modules:

Step 1 Configure the asynchronous group interface.

Step 2 Configure the modems.

Step 3 Configure modem pooling.

Step 4 Configure the controllers.

Step 5 Configure the serial interfaces.

Step 6 Configure R2 signaling.

Configuring the Asynchronous Group Interface

Use the following table to configure the asynchronous group interface. You can assign the asynchronous interfaces to a group so that you can configure them as a group, instead of individually. Use the commands in Table 6 to configure the asynchronous group interfaces.

Timesaver Because there are so many asynchronous interfaces on the access server, configuring them as a group will save you time.

Table 6 Configuring the Asynchronous Group Interface

Step	Command	Purpose
1	5200> **enable** Password: <*password*> 5200#	Enter enable mode. Enter the password. You have entered enable mode when the prompt changes to 5200#.
2	5200# **config term** Enter configuration commands, one per line. End with CNTL/Z. 5200(config)#	Enter global configuration mode. You have entered global configuration mode when the prompt changes to 5200(config)#.
3	5200(config)# **interface group-async 1** 5200(config-if)#	Place all asynchronous interfaces in a single group, so that you configure the same parameters quickly on all interfaces at one time.
4	5200(config-if)# **ip unnumbered ethernet 0**	To conserve IP addresses, configure the asynchronous interfaces as unnumbered and assign the IP address of the Ethernet interface to them.
5	5200(config-if)# **encapsulation ppp**	Enable PPP to run on the set of interfaces in the group.
6	5200(config-if)# **async mode interactive**	Configure interactive mode on the asynchronous interface.
7	5200(config-if)# **ppp authentication chap pap**	Enable CHAP and PAP authentication on the interface.
8	5200(config-if)# peer default ip address pool default	Support dial-in PC clients. At the global level, define the pool of addresses.
9	5200(config-if)# **group-range 1 48** Building configuration... 5200(config-if)#	Define the group range of the interface. The number you use with the **group-range** command depends on the number of asynchronous interfaces you have on your access server. That is, if your access server has 48 asynchronous interfaces, you can specify **group-range 1 48**. If 60, specify **group-range 1 60**.

Table 6 Configuring the Asynchronous Group Interface (Continued)

Step	Command	Purpose

10	`5200(config-if)# end`
	`5200#`
	`%SYS-5-CONFIG_I: Configured from console by console`
	`5200#`
		Return to enable mode.
		
		This message is normal and does not indicate an error.

Verify

To verify your group interface configuration, use the following command.

- Enter the **show interface async** command:

```
5200# show interface async 1
Async1 is up, line protocol is up
modem(slot/port)=1/0, csm_state(0x00000204)=CSM_IC4_CONNECTED, bchan_num=18
modem_status(0x0002): VDEV_STATUS_ACTIVE_CALL.

  Hardware is Async Serial
  Interface is unnumbered.  Using address of FastEthernet0 (15.0.0.60)
  MTU 1500 bytes, BW 115 Kbit, DLY 100000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive not set
  DTR is pulsed for 5 seconds on reset
  LCP Open
  Open: IPCP
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/5, 0 drops; input queue 1/5, 0 drops
  5 minute input rate 37000 bits/sec, 87 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     31063 packets input, 1459806 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     33 packets output, 1998 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Tips

Check for errors and the local and remote addresses.

- Enter the **show async status maps** command:

```
5200# show async status maps
Async protocol statistics:
  Rcvd: 27887 packets, 1294133 bytes
        0 format errors, 0 checksum errors, 0 overrun, 0 no buffer
  Sent: 2141 packets, 117673 bytes, 0 dropped

 Int           Local          Remote Qd     InPack     OutPac Inerr  Drops  MTU
*  1       15.0.0.60        50.2.8.1  0        542         35     0      0 1500
*  2       15.0.0.60        50.3.8.1  0        544         35     0      0 1500
*  3       15.0.0.60       100.2.1.1  0        542         35     0      0 1500
*  4       15.0.0.60        50.1.1.1  0        544         35     0      0 1500
*  5       15.0.0.60        99.2.7.1  0        542         34     0      0 1500
*  6       15.0.0.60        99.1.4.1  0        543         34     0      0 1500
*  7       15.0.0.60       100.2.3.1  0        451         34     0      0 1500
*  8       15.0.0.60       100.2.5.1  0        451         34     0      0 1500
*  9       15.0.0.60       100.2.6.1  0        452         34     0      0 1500
```

```
* 10       15.0.0.60       100.2.8.1  0        452         34     0      0 1500
* 11       15.0.0.60        30.2.6.1  0        449         34     0      0 1500
* 12       15.0.0.60        30.3.5.1  0        450         34     0      0 1500
* 13       15.0.0.60        30.2.4.1  0        450         34     0      0 1500
* 14       15.0.0.60        30.2.8.1  0        450         34     0      0 1500
  15       15.0.0.60            None  0          0          0     0      0 1500
* 16       15.0.0.60        50.3.5.1  0        355         27     0      0 1500
```

- For other async debugging commands, enter the **debug ppp negotiation** and **debug ppp authentication** commands.

```
5200# debug ppp negot
5200# debug ppp authen

    Mar 28 15:40:40.963: ppp: sending CONFREQ, type = 2 (CI_ASYNCMAP), value = 0xA0000
    Mar 28 15:40:40.967: ppp: sending CONFREQ, type = 3 (CI_AUTHTYPE), value = 0xC023
    Mar 28 15:40:40.967: ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value =
    0xC9BAE6A0
    Mar 28 15:40:41.091: PPP Async1: state = REQsent fsm_rconfack(0xC021): rcvd id 3
    Mar 28 15:40:41.095: ppp: config ACK received, type = 2 (CI_ASYNCMAP), value =
    0xA0000
    Mar 28 15:40:41.099: ppp: config ACK received, type = 3 (CI_AUTHTYPE), value =
    0xC023
    .
    .
    .
```

Configuring the Modems

Configure the modems to allow users to dial in to your network by using the commands in Table 7.

Table 7 Configuring the Modems

Step	Command	Purpose
1	5200> **enable** Password: <*password*> 5200#	Enter enable mode. Enter the password. You have entered enable mode when the prompt changes to 5200#.
2	5200# **config term** Enter configuration commands, one per line. End with CNTL/Z. 5200(config)#	Enter global configuration mode. You have entered global configuration mode when the prompt changes to 5200(config)#.
3	5200(config)# **modem country mica** *country name*	Specify the country to set the modem parameters (including country code and encoding) for MICA modems. The default is **usa** if the access server is configured with T1 interfaces and **e1-default** if the access server has E1 interfaces. For list of country codes, see "Country Code Tables" later in this section.
4	5200(config-if)# **line 1 48** 5200(config-line)#	Enter the number of modem lines to configure. If you have 48 modems, enter **line 1 48**. If 60, enter **line 1 60**.
5	5200(config-line)# **transport input all**	Allow all protocols to be used when connecting to the line.
6	5200(config-line)# **autoselect ppp**	Enable remote IP users running a PPP application to dial in, bypass the EXEC facility, and connect directly to the network.
7	5200(config-line)# **modem inout**	Enable incoming and outgoing calls.

Table 7 Configuring the Modems (Continued)

Step	Command	Purpose

8	`5200(config-line)# end`
	`5200#`
	`%SYS-5-CONFIG_I: Configured from console by console`
	`5200#`
		Return to enable mode.
		
		This message is normal and does not indicate an error.

Country Code Tables

Table 8 lists the current MICA modem codes.

Table 8 MICA Modem Codes

Country	Code	Country	Code
Australia	`australia`	Netherlands	`netherlands`
Austria	`austria`	New Zealand	`new-zealand`
Belgium	`belgium`	Norway	`norway`
China	`china`	Poland	`poland`
Cyprus	`cyprus`	Portugal	`portugal`
Czech/Slovak Republic	`czech-republic`	Russia	`russia`
Denmark	`denmark`	Singapore	`singapore`
Default E1 (A Law)	`e1-default`	South Africa	`south-africa`
Finland	`finland`	Spain	`spain`
France	`france`	Sweden	`sweden`
Germany	`germany`	Switzerland	`switzerland`
Hong Kong	`hong-kong`	Default T1 (u Law)	`t1-default`
India	`india`	Taiwan	`taiwan`
Ireland	`ireland`	Thailand	`thailand`
Israel	`israel`	Turkey	`turkey`
Italy	`italy`	United Kingdom	`united-kingdom`
Japan	`japan`	USA	`usa`
Malaysia	`malaysia`		

To reset to default settings for country codes, enter the following commands in global configuration mode:

- **no modem country mica**—Resets to default MICA setting.

Configuring Modem Pooling

Use modem pooling to define, select, and use separate pools of modems within a single access server to enable different dial-in services for different customers. The primary application is to allocate specific modems based on called party numbers and a predetermined number of modem ports based on Dialed Number Information Service (DNIS).

If you do not configure any modem pools, all the modems are placed into a single pool. There is no restriction on the number of modem pools that you can configure. A pool can contain a minimum of one modem and a maximum equal to all the modems in the system.

This section briefly shows how to set up a minimum configuration. For detailed information on using this feature, refer to the command reference documents shipped with your access server.

Note To support modem pooling over channelized T1 lines, you need to configure the lines as described in the following table. If you are using R2 signaling over channelized E1, you do not need any special configuration options since DNIS information is always collected.

Table 9 Configuring Modem Pooling

Step	Command	Purpose

1	`5200> enable`
	`Password: <password>`
	`5200#`
		Enter enable mode.
		Enter the password.
		You have entered enable mode when the prompt changes to `5200#`.

2	`5200# configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`5200(config)#`
		Enter global configuration mode. You have entered global configuration mode when the prompt changes to `5200(config)#`.

3	`5200(config)# controller [t1 | e1] [0 | 1 ]` `5200(config-controller)#`	Enter controller configuration mode to configure your controller port. The controller ports are labeled 0 through 1 on the T1/PRI and E1/PRI cards.
4	`5200(config-controller)# cas-group 1 timeslots [1-24 | 1-31] <type>`	Configure all channels for E&M, FXS, and SAS analog signaling. Enter **1-24** for T1. If E1, enter **1-31**. Signaling types include **e&m-fgb**, **e&m-fgd**, **e&m-immediate-start**, **fxs-ground-start**, **fxs-loop-start**, **sas-ground-start**, and **sas-loop-start**. **Note:** To set up e&m-fgb to support modem pooling, see step 8 in this table. You must use the same type of signaling that your central office uses. For E1 using the Anadigicom converter, use **cas e&m-fgb** signaling.

Table 9 Configuring Modem Pooling (Continued)

Step	Command	Purpose
5	5200(config-controller)# **cas-group 1 timeslots 1-24 e&m-fgb mf dnis** [or] 5200(config-controller)# **cas-group 1 timeslots 1-24 e&m-fgb dtmf dnis**	Configure **e&m-fgb** signaling to support modem pooling and the digital number identification service (DNIS) over channelized T1 lines. You must specify the tone type: **mf** or **dtmf**. By configuring DNIS as part of the **cas-group** command, the system collects DNIS digits for incoming calls, which are redirected to specific modem pools. You must be running MICA modems in the system and have at least 10% of your total modems in the default modem pool. Free modems are needed in the default pool to detect the incoming called number or DNIS before handing the call off to the appropriate modem pool. Therefore, a second modem is needed to handle each incoming call. **Note:** Make sure your switch provides inband address information for incoming analog calls before you enable this feature.
6	5200(config-controller)# **controller t1 1** 5200(config-controller)# **cas-group 2 timeslots 1-24 e&m-fgb mf dnis** [or] 5200(config-controller)# **cas-group 2 timeslots 1-24 e&m-fgb dtmf dnis**	Repeat Steps 3 to 5 to configure the second controller. In this example, note that the controller number is 1, instead of 0. And the cas-group is 2, instead of 1.
7	5200(config)# **modem-pool** *name*	Enter the name of the modem to configure for pooling.
8	5200(config-modem-pool)# **pool-range** *number-number*	Define the range of the modems in the pool. A dash is required between the two numbers.
9	5200(config-modem-pool)# **called number** *phone #* **max-conn** *number*	Specify the DNIS to be used for this modem pool. The DNIS string can have an integer *x* to indicate a don't care digit for that position. The **max-conn** option specifies the maximum number of connections allowed for this DNIS. If you do not specify a **max-conn value**, the default (total number of modems in the pool) is used. The **max-conn** values can range from one to the total number of modems in the pool.
10	5200(config-modem-pool)# **Ctrl-Z** 5200#	Return to enable mode.

Verify

To verify your modem pooling configuration:

- Enter the **show modem-pool** command to view information for all modem pools. To view information for a specific modem pool, enter the **show modem-pool** *name* command.

```
5200# show modem-pool
modem-pool: System-def-Mpool
modems in pool: 60 active conn: 0
 0 no free modems in pool

modem-pool: test
modems in pool: 1 active conn: 0
 0 no free modems in pool
called_party_number: 1000
  0 max-conn exceeded, 0 no free modems in pool
```

Tips

If you are having trouble:

- Make sure you have not configured the same called party number for multiple pools.
- Make sure you have not placed modems in multiple pools.

Configuring the Controllers

Use Table 10 to configure the controllers.

Table 10 Configuring the Controller

Step	Command	Purpose
1	5200(config)# **isdn switch-type primary-5ess**	Enter your telco's switch type. The following switch types are available: primary-4ess, primary-5ess, primary-dms100, primary-net5, primary-ntt, and primary-ts014.
2	5200(config)# **controller t1 0** [or] 5200(config)# **controller e1 0** 5200(config-controller)#	Enter controller configuration mode to configure your controller port. On the Cisco AS5200, the controller ports are labeled 0 and 1 on the dual T1/PRI and dual E1/PRI cards.
3	5200(config-controller)# **framing esf**	Enter your telco's framing type. The following framing types are available: esf, sf, crc4, and nocrc4.
4	5200(config-controller)# **linecode b8zs**	Enter your telco's line code type. The following line code types are available: ami, b8zs, and hdb3.
5	5200(config-controller)# **clock source line primary**	Enter the clock source for the line. Configure one line as the primary or most stable clock source line. Configure the other line as the secondary clock source line.

Table 10 Configuring the Controller (Continued)

Step	Command	Purpose
6	5200(config-controller)# **pri-group timeslots 1-24** [or] 5200(config-controller)# **pri-group timeslots 1-31**	Configure all channels for ISDN. Enter **pri-group timeslots 1-24** for T1. If E1, enter **pri-group timeslots 1-31**.
7	5200(config-controller)# **controller t1 1** [or] 5200(config)# **controller e1 0** 5200(config-controller)# **framing esf** 5200(config-controller)# **linecode b8zs** 5200(config-controller)# **clock source line secondary** 5200(config-controller)# **pri-group timeslots 1-24** [or] 5200(config-controller)# **pri-group timeslots 1-31**	Repeat steps 2 to 6 to configure subsequent controllers. Note that the controller number is 1, 2, or 3, instead of 0. And the clock source is secondary, instead of primary.
8	5200(config-controller)# **Ctrl-Z** 5200#	Return to enable mode.

Configuring the Serial Interfaces

Use Table 11 to configure the serial interfaces.

Table 11 Configuring the Serial Interfaces

Step	Command	Purpose
1	5200(config-controller)# **interface serial0:23** 5200 (config-if)#	Enter serial interface configuration mode. After you have configured the controller, a corresponding D-channel serial interface is created instantly. Serial interface 0:23 is the D-channel for controller 0. You must configure each serial interface to receive incoming and send outgoing modem signaling.
2	5200(config-if)# **isdn incoming-voice modem**	Configure all incoming voice calls to go to the modems.
3	5200(config-if)# **end** 5200#	Return to enable mode.
	%SYS-5-CONFIG_I: Configured from console by console <**Return**> 5200#	When this message appears, press **Return** to get the 5200# prompt.
4	5200# **copy running-config startup-config** Building configuration... [OK] <**Return**> 5200#	Save the configuration changes to NVRAM.

Configure R2 Signaling

R2 signaling is an international signaling standard that is common to channelized E1 networks. You can configure a channelized E1 interface to support different types of R2 signaling, which is used in older analog telephone networks. Note that this feature is available for MICA modems. UseTable 12 to configure R2 signaling.

Table 12 Configure R2 Signaling

Step	Command	Purpose
1	5200> **enable** Password: **<*password*>** 5200#	Enter enable mode. Enter the password. You have entered enable mode when the prompt changes to 5200#.
2	5200# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. 5200(config)#	Enter global configuration mode. You have entered global configuration mode when the prompt changes to 5200(config)#.
3	5200(config)# **controller e1** [**0** | **1**] 5200(config-controller)#	Enter controller configuration mode to configure your E1 controller port. The E1 controller ports are labeled 0 and 1 on the E1/PRI cards.
4	5200(config-controller)# **framing crc4** [or] 5200(config-controller)# **framing no-crc4**	Configure framing to E1 with CRC[1]. Configure framing to E1 only.
5	5200(config-controller)# **linecode ami** [or] 5200 (config-controller)# **linecode hdb3**	Configure line code to AMI[2] encoding. Configure line code to HDB3[3] encoding.
6	5200(config-controller)# **clock source internal** [or] 5200(config-controller)# **clock source line primary** [or] 5200(config-controller)# **clock source line secondary**	Configure the clock source to the internal clock. Configure the clock source to the primary recovered clock. Configure the clock source to the secondary recovered clock.
7	5200(config-controller)# **cas-group 1 timeslots 1-30 type r2-analog r2-compelled ani**	Configure the timeslots that belong to each E1 circuit for R2 signaling. Sets R2 signaling to R2 ITU Q411, the tone signal to R2 Compelled Register Signaling, and the ANI addr info provisioned option. R2 line signaling options include: **r2-analog**, **r2-digital, and r2-pulse**. Tone signaling options include **dtmf** (default), **r2-compelled**, **r2-non-compelled**, and **r2-semi-compelled**. You can also set **ani** (ANI addr info provisioned) for any of the above options.
8	5200(config-controller-cas)# **cas-custom 1**	Enter the channel number to customize.

Table 12 Configure R2 Signaling (Continued)

Step	Command	Purpose
9	`5200(config-ctrl-cas)# country` *country name* `use-default`	Use defaults for the specified country. Note: To view the parameters for the country (if the country defaults are the same as ITU defaults), enter **write term**. The default setting for all countries is **ITU**. See "Country Codes for R2 Signaling" later in this section for a list of supported countries.
10	`5200(config-ctrl-cas)# answer-signal group-b 6`	Set the cas custom command answer-signal to group-b to 6. Cas custom commands include: **caller-digits**, **category**, **country**, **unused-abcd**, **invert-abcd**, **metering**, **ka**, **kd**, **dnis-digits**, **answer-signal**, and **nc-congestion**.
	`[or]` `5200(config-ctrl-cas)# default answer-signal group-b 6`	Set answer-signal group-b to the default ITU value.
	`[or]` `5200(config-ctrl-cas)# no answer-signal group-b 6`	Reset answer-signal group-b 6 to the default value. **Note:** The parameters you do not set are automatically set to the ITU default by the Cisco AS5200.

	`controller E1 0`
	` clock source line primary`
	` cas-group 0 timeslots 1-15,17-31 type r2-analog`
	` r2-compelled`
	` cas-custom 0`
	`  country singapore use-defaults`
	`  category 2  <--- default category for singapore`
	`  answer-signal group-b 6   <--- default bxfree`
	`  for singapore`
		After you configure a country with default settings, the Cisco AS5200 displays a write term, similar to the one displayed here.

	`5200(config-ctrl-cas)# exit`	Exit the cas-custom mode.

11	`5200(config-if)# Ctrl-Z`
	`5200#`
	`%SYS-5-CONFIG_I: Configured from console by console`
		Return to enable mode.
		This message is normal and does not indicate an error.

1. CRC = Cyclic Redundancy Check.
2. AMI = Alternate Mark Inversion.
3. HDB2 = Line code type used on E1 circuits.

Country Codes for R2 Signaling

Table 13 lists the country codes supported for R2 signaling.

Table 13 Country Codes for R2 Signaling

Country	Code
Argentina	argentina
Australia	australia
Brazil	brazil
China	china
Columbia	columbia
Costa Rica	costarica
East Europe	easteurope
Ecuador ITU	ecuador-itu
Ecuador LME	ecuador-lme
Greece	greece
Guatemala	guatemala
Hong Kong (China variant)	hongkong-china
Indonesia	indonesia
Israel	israel
ITU (default)	itu
Korea	korea
Malaysia	malaysia
New Zealand	newzealand
Paraguay	paraguay
Peru	peru
Philippines	philippines
Saudi Arabia	saudiarabia
Singapore	singapore
South Africa Panafte	southafrica-panaftel l
Telmex	telmex
Telnor	telnor
Thailand	thailand
Uruguay	uruguay
Venezuela	venezuela
Vietnam	vietnam

Verify

To verify your R2 signaling configuration:

- Enter the **show controller e1** command to view the status for all controllers, or enter the **show controller e1 #** to view the status for a particular controller. Make sure the status indicates the controller is up (line 2 in the following example) and no alarms (line 4 in the following example) or errors (lines 9 and 10 in the following example) have been reported.

```
5200# show controller e1 0
E1 0 is up.
  Applique type is Channelized E1 - balanced
  No alarms detected.
  Version info of Slot 0:  HW: 2, Firmware: 4, PLD Rev: 2

Manufacture Cookie is not programmed.

  Framing is CRC4, Line Code is HDB3, Clock Source is Line Primary.
  Data in current interval (785 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 13 15 minute intervals):
     0 Line Code Violations, 0 Path Code Violations,
     0 Slip Secs, 12 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 12 Unavail Secs
```

- Enter the **show modem csm [***slot/modem-port***]** command to view status for a specific modem:

```
5200# show modem csm 1/0
MODEM_INFO: slot 1, port 0, unit 0, tone r2-compelled, modem_mask=0x0000,
modem_port_offset=0
tty_hwidb=0x60E63E4C, modem_tty=0x60C16F04, oobp_info=0x00000000, modem_pool=0x60BC60CC
modem_status(0x0002): VDEV_STATUS_ACTIVE_CALL.
csm_state(0x0205)=CSM_IC5_CONNECTED, csm_event_proc=0x600CFF70, current call thru CAS
line
invalid_event_count=0, wdt_timeout_count=0
wdt_timestamp_started is not activated
wait_for_dialing:False, wait_for_bchan:False
pri_chnl=TDM_PRI_STREAM(s0, u3, c7), modem_chnl=TDM_MODEM_STREAM(s1, c0)
dchan_idb_start_index=0, dchan_idb_index=0, call_id=0x0239, bchan_num=6
csm_event=CSM_EVENT_DSX0_CONNECTED, cause=0x0000
ring_no_answer=0, ic_failure=0, ic_complete=3
dial_failure=0, oc_failure=0, oc_complete=0
oc_busy=0, oc_no_dial_tone=0, oc_dial_timeout=0
remote_link_disc=2, stat_busyout=2, stat_modem_reset=0
oobp_failure=0
call_duration_started=00:04:56, call_duration_ended=00:00:00,
total_call_duration=00:01:43
The calling party phone number =
The called party phone number  = 9993003
total_free_rbs_timeslot = 0, total_busy_rbs_timeslot = 0,
total_dynamic_busy_rbs_timeslot = 0, total_static_busy_rbs_timeslot = 0,
min_free_modem_threshold = 0
```

Tips

If you are having trouble, enable the modem management Call Switching Module (CSM) debug mode using the following command.

- Enter the **debug modem csm** command.

  This is the output of **debug modem csm** for an incoming call:

```
5200# debug modem csm 1/0
*May 15 04:05:46.675: VDEV_ALLOCATE: slot 2 and port 39 is allocated.

*May 15 04:05:46.675: CSM_RX_CAS_EVENT_FROM_NEAT:(04BF):  EVENT_CALL_DIAL_IN at slot 2
and port 39

*May 15 04:05:46.675: CSM_PROC_IDLE: CSM_EVENT_DSX0_CALL at slot 2, port 39
```

```
*May 15 04:05:46.675: Mica Modem(2/39): Configure(0x0)
*May 15 04:05:46.675: Mica Modem(2/39): Configure(0x3)
*May 15 04:05:46.675: Mica Modem(2/39): Configure(0x6)
*May 15 04:05:46.675: Mica Modem(2/39): Call Setup
*May 15 04:05:46.891: Mica Modem(2/39): State Transition to Call Setup
*May 15 04:05:46.891: Mica Modem(2/39): Went offhook
*May 15 04:05:46.891: CSM_PROC_IC1_RING: CSM_EVENT_MODEM_OFFHOOK at slot 2, port 39
.
.
.
```

When the E1 controller comes up, you will see the following messages:

```
%CONTROLLER-3-UPDOWN: Controller E1 0, changed state to up

It also shows these messages for individual timeslots:

%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 1 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 2 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 3 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 4 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 5 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 6 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 7 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 8 is up
.
.
.
```

Configuring New Features

For details on configuring new features available after the release of this document, see the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5200/52spares/index.htm

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com

- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

CD-ROM/WWW Feedback

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar, select **Documentation**, and click **Enter the feedback form**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

This document is to be used in conjunction with the *Regulatory Compliance and Safety Information* publication.

9802R